Claims

What is claimed is:

1. A secure method for generating digital documents that are certified by a known authority, comprising the steps of:

A. Programming an electronic device with a document issuing method that originates with the known authority, wherein the device further includes means for protecting the programmed method from tampering with;

B. programming the electronic device with data identifying the owner of the device, and wherein the device includes means to prevent subsequent alterations of the owner identification data;

C. reading a digital document into the device;

D. physical identification of the owner of the device, based on the identifying data as programmed in step (B);

E. if the result of the identification process in step (D) is positive, this indicating that the true owner requested the document, then issuing of a digital document signed by the known authority, wherein the document is prepared according to the document issuing method that was programmed into the device in step A.

2. The secure method of claim 1, wherein in step A the programming further includes information that is unique to each device.

3. The secure method of claim 1, wherein in step B the device reads a prior issued digital document that attests to a prior identification of the user, and wherein the information in that document is used for programming the electronic device with data identifying the owner of the device.

4. The secure method of claim 1, wherein in step C the device reads a digital document relating to the owner of the device, and further including the step of verifying whether the identifying information in the document corresponds to the owner identification data entered in step B; proceeding to step D only if the identification result is positive, otherwise End procedure.

5. The secure method of claim 1, wherein in step C the device reads a digital document sent to the owner of the device, and further including the step of verifying whether the addressee identity information in the document corresponds to the owner identification data entered in step B; proceeding to step D only if the identification result is positive, otherwise End procedure.

6. The secure method of claim 1, wherein in step E the issued digital document is output through a communication channel in the device.

7. The secure method of claim 1, wherein in step E the issued digital document is stored in digital storage means in the device.

8. The secure method of claim 1, wherein in step E the issued digital document is a permit or a certificate.

9. A device for generating digital documents that are certified by a known authority, comprising:

A. computer means with processing means and memory means for implementing a program written in the memory, and wherein the memory includes a document issuing method that originates with the known authority and data identifying the owner of the device;

B. means for protecting the document issuing method from tampering with;

C. means for preventing subsequent alteration of the owner identifing data;

D. input means for reading information related to physical user identification; and

E. output means for transmitting digital documents generated in the computer means.

10. The device of claim 9, further including means for storing a plurality of digital documents and for retrieving any document as desired.

11. The device of claim 9, further including an input/output channel for receiving documents or user's commands and for outputting digital documents as desired.

12. The device of claim 9, wherein the device is stored in a wristwatch.

13. The device of claim 9, wherein the device is stored in a smart device.